SENETAS

Cyber In Space: The Good, The Bad And The Ugly

SPACE INDUSTRY CYBER THREATS AND SOLUTIONS

THE GOOD: SPACE INDUSTRY CRITICAL INFRASTRUCTURE

The space industry is not simply another industry vertical. It is a fast growing (>7% per annum) component of critical national infrastructure that adds value to many other industries. Growth is driven by its technologies, increasing investment by the public and private sectors and international partnerships. The economic prospects for the industry are best illustrated in the Space Foundation's estimation that the global space industry reached US$428 billion in 2020. The World Economic Forum estimates the global space industry may be worth US$1.8 trillion by 2035.

The critical importance of the space industry to economies reaches throughout the national infrastructure - from defence forces to telecommunications and every industry relied upon. The space industry's broader indirect GDP impact includes its role driving innovation, creating high-skilled jobs, and supporting economic growth in related industries. It is a critically important industry. The space industry's importance demands state-of-the-art cybersecurity.

The space industry's growth is not just a good news story. It is an important story about the industry's contribution to our critical national infrastructure. It supports industries such as telecommunications, agriculture, logistics, aviation and mining through services such as communications, imagery and location positioning. Space industry capabilities are essential to weather forecasting, vegetation and land use monitoring, national security, emergency services, and surveying and mapping.

There are important uses in government agencies, such as Geoscience Australia's internationally recognised Digital Earth publishing data derived from space. There is even a new capability to manoeuvre and manage space debris through the work of the SpaceEnvironment Research Centre.

That is a lot of economic good to protect from cyber threats and bad actors seeking to steal technologies and data as well as to harm space operations and services.

SPACE INDUSTRY IS NOT IMMUNE TO CATASTROPHIC CYBER-ATTACKS

The space industry's complex mix of meshed data networks and interconnected data, software, and working with other connected devices to communicate and compute expose it to catastrophic harm. Increasing data communication in space provides an infinite number of attack surfaces exposing countries economic, national infrastructure, and defence security interests to increasing cybersecurity vulnerabilities. Due to its rapid development of technologies and the significant economic, defence and scientific nature of its space missions, the space industry faces serious cyber threats and persistent cyber attacks by a range of bad actor types. It is a high value target with vulnerabilities that must be addressed to avoid catastrophic harm to space assets, launch controls, missions and communications systems. Vulnerabilities primarily arise from:

1. **Failures to implement risk management-based cybersecurity strategies. Both cyber-attack likelihood and the impact severity rate are high risk factors that demand high levels of priority and cybersecurity investment to ensure preparedness and resilience.**

2. **Space organisations' use of complex data networks due to their many interconnected systems, such as satellites, ground assets, communication networks and datacentres. Space missions and asset management involve mixed data network protocols and complex topologies. These complexities increase their vulnerabilities.**

3. **Dependence upon legacy IT and cybersecurity systems that may not have been designed with current cybersecurity risks in mind, exposing them to greater threats.**

4. **Supply chains expose the industry to countless cyber vulnerabilities. The industry relies on the global supply chains for components, technologies and services. Suppliers and partners may introduce cybersecurity vulnerabilities through compromised systems /products/services.**

5. **People pose a significant risk to space organisations' cybersecurity. Behaviours among employees, contractors, suppliers, and/or partners with access to systems and sensitive data may inadvertently or maliciously compromise cybersecurity.**

Addressing these issues requires an holistic and strategic risk management approach, including investments in risk assessments, cyber defences, people, training, technology and a 'cybersecurity first' culture. Cybersecurity must be seen as fundamental to business operations and space missions to safeguard critical assets, protect sensitive/valuable data, and protect space missions and other operations.

THE BAD: CYBER THREAT LANDSCAPE

In addition to the advancements and benefits the space industry provides countries' critical national infrastructure and faces increasing cybersecurity challenges and threats. When examining cyber threats to the industry, it is also important to consider the attack experiences in the US and EU space industries due to their greater industry sizes and attraction to bad actors— existing and emerging vulnerabilities—the bad and the ugly!

Globally, space industries have increasingly become high-value cyber-attack targets of lone wolf, state-sponsored and criminal syndicates. Moreover, each bad actor type has become significantly more sophisticated and well resourced. There are no rules. How then does cybersecurity deal with such threats?

The answer is threefold. It begins with 'security-first principles'. A cybersecurity strategy that includes a mix of cyber policies, risk assessments, resourcing and investment commitments to threat identification, threat prevention and data protection. It is not sufficient to simply 'tick boxes' or stick to the 'same old' security technologies that are proven not to be resilient to today's persistent and much more sophisticated threat technologies. Thirdly, no organisation should just rely on vendors' security patch updates adding vulnerabilities, costs and systems' downtime. The frequency of IT vendors' security patches is indicative of their products' security weaknesses.

Australia's director general of the Australian Security and Intelligence Organisation (ASIO), Mike Burgess stated that "encryption enables our economy", reflecting on encryption's critical role in data protection throughout the economy—from citizen privacy to protection of intellectual property (IP), defence and government secrets.

Space industry organisations have many attack surfaces exposing their space and ground assets and space operations to significant cyber threats.

Space missions generate huge volumes of valuable data, including telemetry, scientific observations and military and space operational information. Attack surface vulnerabilities risk catastrophic harm:

1. **Unencrypted IT&T and OT communication networks carrying satellite and other data and mission/asset operation controls.**

2. **Denial of service attacks on mission critical networks, such as satellite communication networks and navigation systems, denying critical services, including telecommunications, GPS navigation and weather forecasting, with mission consequences.**

3. **State-sponsored and commercial competitor espionage (e.g., network eavesdropping) or sabotage attacks to gain an advantage or harm space capabilities, thus even posing a threat to national security.**

4. **Supply chain cybersecurity flaws exposing space organisations (and the industry) to vulnerabilities, such as in technologies and assets supplied.**

5. **Weaknesses in access and control systems enabling hackers to gain unauthorised access to satellite systems, or other space assets, potentially disrupting critical communication networks, harming missions or even exposing sensitive data to theft.**

Obviously, direct and indirect costs of successful cyber-attacks to the global industry range from enormous to eye-watering. NASA has been targeted, including attempts to compromise mission-critical systems and steal sensitive data. Consequently, NASA implemented robust end-to-end network encryption protocols; performs regular cyber-drills; and collaborates with government agencies and industry partners to share threat intelligence and best practice cybersecurity.

Cyber-attacks on the European Space Agency (ESA) include its satellite communication networks and other assets. Since then it has adopted strict cybersecurity policies such as end-to-end encryption, threat detection, incident response planning and secure supply chain practices.

However, the US and EU space industries continue to face relentless cyber-attacks, demanding increased vigilance and investment in state-of-the-art cybersecurity. In the eyes of bad actors, the riches are too great to ignore—from data and IP theft to sabotage and operational disruption.

US and EU space industries have experienced supply chain vulnerabilities that bad actors exploited to infiltrate space systems and harm mission-critical operations. Reported serious successful cyber-attacks on US and EU space assets and operations include:

- **In 2018, NASA data breach. Unauthorised individuals accessed one of its servers containing personally identifiable information.**
- **In 2019, NASA's Jet Propulsion Laboratory. Hackers breached the agency's data network gaining access to sensitive data about space missions and Mars exploration projects.**
- **In 2019, the US Department of Defense reported supply chain vulnerabilities in space industry satellite components. This highlighted risks to national security.**
- **In 2020, the ESA disclosed a data breach on its ExoMars mission exploring Mars for signs of life. Its network was breached compromising sensitive scientific mission data. Space industries are prime targets for espionage and state-sponsored cyber-threats aimed at stealing IP, gaining a strategic advantage or disrupting/denying space activities. The strategic importance of space assets highlights the criticality of state-of-the-art cyber defences.**

As other industries' reliance on space technologies (e.g., satellite communications) increases, addressing cybersecurity vulnerabilities remains the critical imperative for ensuring the integrity, resilience and security of space exploration efforts.

THE UGLY: WEAPONISED QUANTUM COMPUTING

The expected computational power of quantum computers holds enormous potential for the space industry by enabling advanced data analytics, simulations and modelling, spacecraft design optimisation, enhanced sensing and navigation.

However, quantum computing in the hands of bad actors also presents new and greater cybersecurity risks, causing implications that are being addressed by regulators (e.g., the US Quantum Computing Cybersecurity Preparedness Act, 2020).

By harnessing the benefits of quantum computing while preventing its threats, the space industry will unlock new opportunities in space exploration and scientific discovery.

Quantum computing, with its quantum mechanics-based information processing holds great promise for transforming space exploration. However, along with its benefits come significant threats that must be addressed in any space organisation's cybersecurity strategy and cybersecurity solutions.

The threats of quantum computing to conventional mathematics-based cryptography, public encryption key infrastructure and communications protocols requires quantum-safe encryption. Simply, cybersecurity solutions must be 'quantum safe'. Quantum-safe encryption components are:

1. **Quantum resistant algorithms**
2. **Quantum key distribution**
3. **Quantum random number generation**

Cybersecurity risks arise from quantum computing's ability to break existing conventional encryption protocols—to decrypt sensitive data transmitted among spacecraft—which threatens mission security and confidentiality. Threats to satellite communications lead to communication blackouts, interference with navigation systems and compromised data transmission.

Quantum-safe encryption will be essential to the future security of space communications and sensitive data transmission among spacecraft, ground stations and mission control as quantum computing becomes weaponised. It is important now because much space industry data is long-life, requiring quantum-safe encryption today to provide long-term protection against future quantum threats.

CIA PRINCIPLES: CONFIDENTIALITY, INTEGRITY AND AVAILABILITY

The CIA (confidentiality, integrity and availability) principles are the foundation of cybersecurity and essential to protecting systems and data from unauthorised access, modification, disruption or theft. An effective cybersecurity strategy will be based on these three principles:

SENETAS

a. **Confidentiality requires information to only be accessible by authorised parties. It prevents unauthorised access, disclosure or theft of sensitive data. Data encryption, access control and secure communication protocols are required.**

b. **Integrity ensures that data remains accurate, complete, and trustworthy throughout its lifecycle, while at rest (stored), in use and in motion across data networks. It requires safeguards to prevent unauthorised data modification, deletion or corruption. Security tools such as encryption, hashing, digital signatures and version control help maintain data integrity and detect unauthorised changes.**

c. **Availability ensures that data is accessible and usable as required. It involves security that prevent business disruptions, downtime or denial of service attacks that will impair access to critical systems.**

As the space industry grows, the risks of cyber-attacks should be a primary business and investment priority. Failure to ensure the cyber resilience of space assets and operations will be enormously damaging financially and reputationally. It is certain cyber-attacks are here to stay.

In any industry, preventing successful cyber-attacks requires proactive cybersecurity strategies and investments in attack prevention and data protection—through threat prevention and surveillance technologies and end-to-end encryption. Importantly, cybersecurity plans should not be limited to preventing cyber-attacks. It must also account for protecting the data in the event of a successful attack. Only end-to-end encryption provides that last line of defence to ensure breached data is useless in the hands of unauthorised parties.

Just as the space industry's technologies and capabilities have grown rapidly, so too have bad actors' weapons. It is a fact of crime that the criminals are always one step ahead.
The looming biggest cybersecurity threat is quantum computing. Like all new technologies that offer significant benefits, in the hands of bad actors weaponised quantum computing is considered by experts to be the biggest cybersecurity threat in history.

This remarkable industry may well experience the good, the bad and the ugly.

ZERO TRUST CYBERSECURITY: PROTECTING ASSETS AND OPERATIONS

Preventing cyber-attacks and protecting space organisations' data require a 'zero trust approach to cybersecurity. The critical cybersecurity strategy features necessary to safeguard space assets and operations are:

1. **'Military-grade' end-to-end encryption protocols for secure and authenticated data transmission (data, voice and video) across all networks and data storage prevents risks of unauthorised access, malware and data breaches. Authenticated end-to-end encryption should be applied across all communication networks—channels, satellite links and ground-based systems. Why military-grade? Because the most secure encrypted networks use authenticated 'end-to-end' encryption technology and recognised security certifications, e.g., FIPS Level 3 (US) and Common Criteria EAL4+ certified (EU) as proven suitable for defence and government use.**

2. **A comprehensive cybersecurity strategy and practices necessary to reduce the likelihood of successful cyber-attacks. Organisations must build a culture of cybersecurity awareness and vigilance. This should include standards specific to the space industry, including business and regulatory compliance requirements.**

3. **Processes to share cyber threat intelligence and cybersecurity best practices within the global space industry.**

4. **Secure supply chains essential to reducing attack surface vulnerabilities. They must include thorough periodic risk assessments and due diligence reviews of suppliers and other vendors and partners. This will enhance industry expectations of security transparency and accountabilities.**

5. **Planned incidence responses and regular cyber drills achieve more effective cyber-attack responses and avoid catastrophes—rather than being caught by surprise.**

GLOBAL SUPPORT

Senetas encryption solutions are distributed and supported internationally (outside Australia and New Zealand) by Thales and within government & defence sectors by Thales Defense & Security Inc.

THALES

Thales is the world leader in digital security and defence, servicing over 30,000 customers across 180 countries.

ANZ PARTNER COMMUNITY

Senetas works directly with customers and their service providers across Australia and New Zealand. We provide technical advice and support to data networks providers, systems integrators and cloud service providers.
For a current list, visit our ANZ Partner Community Page.

© SENETAS CORPORATION LIMITED

www.senetas.com

Senetas is the leading developer of end-to-end encryption security solutions; trusted to protect the world's most sensitive data , from enterprise, government, defence, to Cloud and service provider network data in over 50 countries.

From certified high-assurance hardware and virtualised encryption, to secure file sharing and collaboration with data sovereignty control, all are based on the same crypto-agile platform and deliver security without compromise.

SENETAS
Proudly made in Australia.

GET IN TOUCH

Are you looking for a service provider to help you select and implement a network data encryption or secure file sharing and collaboration solution? Contact Senetas and we'll help you find the right one.

Senetas works with IT infrastructure service providers and systems integrators across the globe, to help specify the optimal cybersecurity solution for their customers' needs.

Customers may contact Senetas directly to discuss their requirements; or ask their service provider to speak to us on their behalf.

NETWORK DATA SECURITY WITHOUT COMPROMISE

Whatever your network security needs, Senetas has a network independent encryption solution to suit all network types. Our multicertified high-assurance encryptors protect data across networks operating at speeds from modest 100Mbps to ultra-fast 100Gbps and support all network topologies.

Our virtualised encryption solution, for virtual CPE and virtualised WAN, supports bandwidths of up to 15Gbps. It provides policy-based, end-to-end encryption across multi-Layer networks.

Senetas encryptors are Quantum resilient and recognised globally for delivering maximum data security and crypto-agility, without compromising network or application performance.

They are trusted to protect the world's most sensitive government, defence and commercial data.

SECURE COLLABORATION

SureDrop offers all the flexibility of a drop-box style solution, with the added benefits of best-in-class encryption security and 100% control over data sovereignty.

DISARM MALICIOUS CONTENT

Votiro Zero Trust leverages patented Content Disarm

& Reconstruction (CDR) technology to protect your files from the most advanced, signatureless, persistent cyber-attacks. It sanitises incoming files, eliminating the risks associated with zero-day or undisclosed attacks, whilst preserving 100% file functionality.

Regional Contacts:

Asia	**T:** +65 8307 3540	**E:** infoasia@senetas.com
Australia & New Zealand	**T:** +61(03) 9868 4555	**E:** info@senetas.com
Europe, Middle East & Africa	**T:** +44 (0)1256 345 599	**E:** infoemea@senetas.com
The Americas	**T:** +1 949 436 0509	**E:** infousa@senetas.com